AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently Amended) A mutual authentication method for use between a recording apparatus which records copied contents on a recording medium having an arithmetic processing function, and the recording medium, said method comprising the steps of:

storing in the recording medium at least first information which depends on the recording medium, and second information which is to be shared by the recording apparatus in executing mutual authentication with the recording apparatus and depends on the recording medium; and

generating by the recording apparatus authentication information used in mutual authentication with the recording medium on the basis of only the first information obtained from the recording medium, and executing mutual authentication between the recording apparatus and the recording medium using the generated authentication information and the second information, wherein executing the mutual authentication includes the steps of

generating a random number in the recording apparatus and transferring the random number to the recording medium,

generating a first function in the recording apparatus using the generated authentication information and the generated random number,

generating a second function in the recording medium using the generated second information and the transferred random number, and transferring the second function to the recording apparatus, and

comparing the generated first function with the generated second function in the recording apparatus.

2. (Original) The method according to claim 1, further comprising the step of:

generating the authentication information by encrypting the first information using an encryption key obtained from the recording medium.

A1

3. (Currently Amended) A mutual authentication method for use between a reproducing apparatus which reproduces copied contents recorded on a recording medium having an arithmetic processing function, and the recording medium, said method comprising the steps of:

storing in the recording medium at least first information which depends on the recording medium, and second information which is to be shared by the reproducing apparatus in executing mutual authentication with the reproducing apparatus and depends on the recording medium; and

generating by the reproducing apparatus authentication information used in mutual authentication with the recording medium on the basis of only the first information obtained from the recording medium, and executing mutual authentication between the reproducing apparatus and the recording medium using the generated

authentication information and the second information, wherein executing the mutual authentication includes the steps of

generating a random number in the reproducing apparatus and transferring the random number to the recording medium,

generating a first function in the reproducing apparatus using the generated authentication information and the generated random number,

generating a second function in the recording medium using the generated second information and the transferred random number, and transferring the second function to the reproducing apparatus, and

comparing the generated first function with the generated second function in the reproducing apparatus.

4. (Original) The method according to claim 3, further comprising the step of:

generating the authentication information by encrypting the first information using an encryption key obtained from the recording medium.

5. (Currently Amended) A recording apparatus for recording copied contents on a recording medium while limiting the number of copied contents to be recorded on the recording medium, said apparatus comprising:

generation means for generating authentication information, which is used in mutual authentication with the recording medium and is to be shared by the recording medium, on the basis of only first information which is obtained from the recording medium and depends on the recording medium; and

mutual authentication means for executing mutual authentication with the recording medium using the authentication information generated by said generation means, wherein the mutual authentication means includes

means for generating a random number and transferring the random number to the recording medium,

means for generating a first function using the generated authentication information and the generated random number,

means for receiving from the recording medium a second function generated using second information and the transferred random number, and

means for comparing the generated first function with the received second function.

6. (Original) An apparatus according to claim 5, wherein said generation means generates the authentication information by encrypting the first information using an encryption key obtained from the recording medium.

7. (Currently Amended) A reproducing apparatus for reproducing copied contents recorded on a recording medium while limiting the number of copied contents to be recorded on the recording medium, said apparatus comprising:

generation means for generating authentication information, which is used in mutual authentication with the recording medium and is to be shared by the recording medium, on the basis of only first information which is obtained from the recording medium and depends on the recording medium; and

mutual authentication means for executing mutual authentication with the recording medium using the authentication information generated by said generation means, wherein the mutual authentication means includes

means for generating a random number and transferring the random number to the recording medium,

means for generating a first function using the generated authentication information and the generated random number,

means for receiving from the recording medium a second function generated using second information and the transferred random number, and

means for comparing the generated first function with the received second function.

8. (Original) An apparatus according to claim 7, wherein said generation means generates the authentication information by encrypting the first information using an encryption key obtained from the recording medium.

9. (Currently Amended) A recording medium having an arithmetic processing function, comprising:

storage means for pre-storing first information which is unique to said recording medium, and second information which is to be shared by a recording apparatus for recording copied contents on said recording medium and a reproducing apparatus for reproducing the copied contents in executing mutual authentication among the

recording medium, the recording apparatus, and the reproducing apparatus, and depends on said recording medium; and

mutual authentication means for executing mutual authentication between the recording medium and the recording apparatus, and between the recording medium and the reproducing apparatus using authentication information generated based on only the first information by the recording apparatus and the reproducing apparatus, and the second information, wherein the mutual authentication means includes

means for generating a random number and transferring the random number to one of the recording apparatus and the reproducing apparatus,

means for generating a first function using the second information and the generated random number,

means for receiving from the one of the recording apparatus and the reproducing apparatus a second function generated using the authentication information and the transferred random number, and

means for comparing the generated first function with the received second function.